RFC 2350 AP1-CSIRT

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi AP1-CSIRT berdasarkan RFC 2350, yaitu informasi dasar mengenai AP1-CSIRT, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi AP1-CSIRT.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal …… 2023.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt[at]ap1.co.id (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Kedua dokumen telah ditandatangani dengan PGP *Key* milik AP1-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 AP1-CSIRT;
Versi : 1.0;
Tanggal Publikasi : …. 2023;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Computer Security Incident Response Team PT. Angkasa Pura I
Disingkat : AP1-CSIRT.

2.2. Alamat

Kantor Pusat – Jakarta
Grha Angkasa Pura I Kota Baru Bandar Kemayoran Blok B12 Kav.2
Jakarta Pusat, DKI Jakarta – Indonesia
Indonesia [10610]

2.3. Zona Waktu

Jakarta (GMT+07:00)

2.4. Nomor Telepon

(021) 6541961 ext.2161

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

Tidak ada

2.7. Alamat Surat Elektronik (*E-mail*)

csirt[at]ap1.co.id

2.8. Kunci Publik (*Public Key*) dan Informasi/Data Enkripsi lain

Bits : 4.096
ID : 1A1A1A12
Key Fingerprint : ……

-----BEGIN PGP PUBLIC KEY BLOCK-----

[pgp_key]
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://websitecsirt.go.id /publickey.asc

2.9. Anggota Tim

Ketua AP1-CSIRT adalah Pejabat Pimpinan Tinggi Pratama dengan bidang tugas teknologi informasi dan komunikasi. Tim AP1-CSIRT adalah Pejabat Administrator, Pejabat Pengawas, Pejabat Fungsional, serta Pelaksana Pengelola Teknologi Informasi dan Komunikasi pada PT. Angkasa Pura I dengan bidang tugas teknologi informasi dan komunikasi.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak AP1-CSIRT

Metode yang disarankan untuk menghubungi AP1-CSIRT adalah melalui *e-mail* pada alamat csirt[at]ap1.go.id.

3. Mengenai AP1-CSIRT

3.1. Visi

Visi AP1-CSIRT adalah mewujudkan pengelolaan keamanan informasi di lingkungan PT. Angkasa Pura I yang sesuai dengan prinsip keamanan informasi yaitu untuk menjamin ketersediaan (*availability*), keutuhan (*integrity*), dan kerahasiaan (*confidentiality*) Aset Informasi PT. Angkasa Pura I.

3.2. Misi

Misi dari AP1-CSIRT, yaitu :

a. Mendorong kegiatan pengamanan informasi dan pencegahan insiden keamanan informasi.
b. Membangun kesadaran keamanan informasi pada sumber daya manusia di lingkungan PT. Angkasa Pura I.
c. Menjamin keamanan informasi pada aset informasi PT. Angkasa Pura I.
d. Melaksanakan evaluasi secara berkala keandalan sistem keamanan teknologi informasi di lingkungan PT. Angkasa Pura I.
e. Meningkatkan kompetensi dan kapasitas sumber daya penanggulangan dan pemulihan keamanan siber di lingkungan PT. Angkasa Pura I.

3.3. Konstituen

Konstituen AP1-CSIRT meliputi PT. Angkasa Pura I dan seluruh kantor cabang

3.4. Sponsorship dan/atau Afiliasi

Rencana Kerja dan Anggaran Perusahaan PT. Angkasa Pura I Republik Indonesia.

3.5. Otoritas

AP1-CSIRT merespon dan melaksanakan penanganan secara teknis terhadap insiden keamanan siber yang terjadi di lingkungan PT. Angkasa Pura I dan unit kerja dibawahnya.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/*Level* Dukungan

AP1-CSIRT memiliki kewenangan untuk menangani berbagai insiden keamanan siber yang terjadi atau yang mengancam konstituen AP1-CSIRT. Dukungan yang diberikan oleh AP1-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

AP1-CSIRT akan menjalin kerja sama dan berbagi informasi dengan CSIRT/organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh AP1-CSIRT akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa AP1-CSIRT dapat menggunakan alamat e-mail dan telepon. Namun, untuk komunikasi yang memuat informasi rahasia dapat menggunakan e-mail yang ter-enkripsi.

5. Layanan

5.1. Layanan Utama

Layanan utama dari AP1-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh AP1-CSIRT berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait layanan ini diberikan oleh AP1-CSIRT

5.1.2. Penanganan Insiden Siber

Layanan ini merupakan layanan teknis terkait penanganan insiden yang terjadi pada konstituen yang meliputi koordinasi, analisis, rekomendasi teknis, dan bantuan on-site jika diperlukan, agar sebuah insiden tidak terulang kembali.

5.2. Layanan Tambahan

Layanan tambahan dari AP1-CSIRT yaitu :

5.2.1. Konsultasi terkait kesiapan penanganan insiden siber

Layanan ini berupa konsultasi terkait kesiapan penanggulangan dan pemulihan insiden yang terjadi di lingkungan PT. Angkasa Pura I dan unit kerja dibawahnya.

5.2.2. Pembangunan kesadaran dan kepedulian terhadap keamanan siber

Layanan ini berupa sosialisasi kepada konstituen AP1-CSIRT yang bertujuan untuk meningkatkan kesadaran dan kepedulian tentang keamanan informasi.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat di input oleh konstituen melalui aplikasi LAPORKAN INSIDEN pada website AP1-CSIRT atau dikirimkan ke alamat csirt[at]ap1.co.id dengan melampirkan :

a. Penjelasan insiden.
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
c. Atau penjelasan tambahan lainnya.

7. *Disclaimer*

Terkait penanganan jenis insiden, menyesuaikan tingkat dan dampak insiden serta ketersediaan perangkat dan sumberdaya yang dimiliki.